VIRUSTOTAL

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Display grouped sandbox reports

Zenbox Linux	0	5	0	0	2	0

Detections

NOT FOUND

Mitre Signatures

6 INFO

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

1 GZIP

Network comms

NOT FOUND

Behavior Tags

detect-debug-environment sets-process-name

MITRE ATT&CK Tactics and Techniques

Search for technique, subtechnique and in its matching entries

None Info

Activity Summary

Download Artifacts Full Reports Help

T1064

T1543

Behavior Similarity Hashes

Zenbox Linux… 532dd8d49eff2a3d52b4084223ac6797

File system actions

Files Opened

/dev/urandom
/etc/dconf/profile/user
/etc/fonts/conf.avail
/etc/fonts/conf.avail/10-antialias.conf
/etc/fonts/conf.avail/10-autohint.conf
/etc/fonts/conf.avail/10-hinting-full.conf
/etc/fonts/conf.avail/10-hinting-medium.conf
/etc/fonts/conf.avail/10-hinting-none.conf
/etc/fonts/conf.avail/10-hinting-slight.conf
/etc/fonts/conf.avail/10-no-sub-pixel.conf

Files Written

/root/.cache/dconf/user

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Files Dropped

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Process and service actions

Processes Created

- /bin/gzip
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
- /usr/bin/exo-open -
- /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
- /usr/bin/systemctl systemctl kill -s HUP rsyslog.service
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate

Shell Commands

- /bin/gzip
- /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh engrampa /tmp/SwissIO_Fixed.zip
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate
- 7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- engrampa /tmp/SwissIO_Fixed.zip
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- systemctl kill -s HUP rsyslog.service

Processes Tree

- 4989 - /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
  - 4991 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
  - 4993 - /usr/bin/exo-open -
- 4994 - /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
  - 4997 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --

close-stderr

5005 - /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip

4942 - /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog

4943 - /usr/lib/rsyslog/rsyslog-rotate

4944 - /usr/bin/systemctl systemctl kill -s HUP rsyslog.service

4945 - /bin/gzip

Highlighted actions

Highlighted Text

""

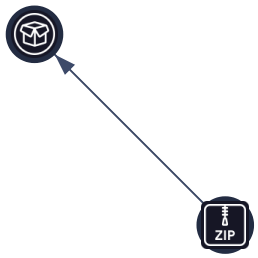
VIRUSTOTAL

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Bundled Files (126)

Scanned	Detections	File type	Name
2026-03-08	0 / 62	Text	SwissIO_Fixed/.git/description
2026-01-18	0 / 60	ZLIB	SwissIO_Fixed/.git/objects/03/d2afd5fe1fb69ca977d620fc564a12b27008aa
2025-12-10	0 / 62	ZLIB	SwissIO_Fixed/.git/objects/d7/b9ef12978379847f8fdf1859d40a76fe1b1b3d
2026-02-28	0 / 62	Perl	SwissIO_Fixed/.git/hooks/fsmonitor-watchman.sample
2026-02-28	0 / 62	Shell script	SwissIO_Fixed/.git/hooks/prepare-commit-msg.sample
2026-02-20	0 / 62	Text	SwissIO_Fixed/.git/HEAD
2026-02-28	0 / 61	Shell script	SwissIO_Fixed/.git/hooks/pre-push.sample
2026-02-28	0 / 62	Shell script	SwissIO_Fixed/.git/hooks/commit-msg.sample
2025-01-12	0 / 60	JavaScript	SwissIO_Fixed/static/addon-fit.min.js
2026-02-28	0 / 62	Shell script	SwissIO_Fixed/.git/hooks/pre-commit.sample

Graph Summary



VIRUSTOTAL

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Basic properties

MD5	a79b00afca60508e415fa5dc3a9a305d
SHA-1	b187edae085cb261493c22ccbaf17cadc97f1a3f
SHA-256	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b9463…
Vhash	86a41950068c7578c98f5737e6223624
SSDEEP	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:E…
TLSH	T16BA4AF30D12E7CEDD49E703521C741E7F3A2D7150126B8CA6…
File type	ZIP compressed zip
Magic	Zip archive data, at least v1.0 to extract, compression method=st…
TrID	ZIP compressed archive (100%)
Magika	ZIP
File size	463.50 KB (474624 bytes)

History

First Submissi…	2026-03-10 00:30:56 UTC
Last Submissi…	2026-03-10 00:30:56 UTC
Last Analysis	2026-03-10 00:30:56 UTC
Earliest Conte…	2026-03-09 20:21:12
Latest Conten…	2026-03-09 20:21:12

Names

SwissIO_Fixed.zip

Bundle Info

Contents Metadata

Contained Fil…	316
Uncompresse…	667.93 KB
Earliest Conte…	2026-03-09 20:21:12
Latest Conten…	2026-03-09 20:21:12

Contained Files By Type

HTML	1
SCRIPT	15
DIRECTORY	129
UNKNOWN	171

Contained Files By Extension

RS	1
LOCK	1
HTML	1
SH	1
TXT	1
CSS	1
JS	2
JSON	2
TOML	2
MD	3
PY	11
SAMPLE	14

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | RELATIONS | BEHAVIOR

Security vendors' analysis	Do you want to automate checks?
Acronis (Static ML)	Undetected
AhnLab-V3	Undetected
Alibaba	Undetected
AliCloud	Undetected
ALYac	Undetected
Antiy-AVL	Undetected
Arcabit	Undetected
Avast	Undetected
Avast-Mobile	Undetected
AVG	Undetected
Avira (no cloud)	Undetected
Baidu	Undetected
BitDefender	Undetected
ClamAV	Undetected
CMC	Undetected
CrowdStrike Falcon	Undetected
CTX	Undetected
Cynet	Undetected
DrWeb	Undetected
Emsisoft	Undetected
eScan	Undetected
ESET-NOD32	Undetected
Fortinet	Undetected
GData	Undetected
Google	Undetected
Gridinsoft (no cloud)	Undetected
Huorong	Undetected
Ikarus	Undetected
Jiangmin	Undetected
K7AntiVirus	Undetected
K7GW	Undetected
Kaspersky	Undetected

Kingsoft	Undetected
Lionic	Undetected
Malwarebytes	Undetected
MaxSecure	Undetected
McAfee Scanner	Undetected
Microsoft	Undetected
NANO-Antivirus	Undetected
Panda	Undetected
QuickHeal	Undetected
Rising	Undetected
Sangfor Engine Zero	Undetected
Skyhigh (SWG)	Undetected
Sophos	Undetected
SUPERAntiSpyware	Undetected
Symantec	Undetected
TACHYON	Undetected
Tencent	Undetected
Trellix ENS	Undetected
TrendMicro	Undetected
TrendMicro-HouseCall	Undetected
Varist	Undetected
VBA32	Undetected
VIPRE	Undetected
VirIT	Undetected
ViRobot	Undetected
Webroot	Undetected
WithSecure	Undetected
Xcitium	Undetected
Yandex	Undetected
Zillya	Undetected
ZoneAlarm by Check Point	Undetected
Zoner	Undetected
Arctic Wolf	Unable to process file type
BitDefenderFalx	Unable to process file type
DeepInstinct	Unable to process file type
Elastic	Unable to process file type
Palo Alto Networks	Unable to process file type
SecureAge	Unable to process file type
SentinelOne (Static ML)	Unable to process file type

Symantec Mobile Insight	Unable to process file type
TEHTRIS	Unable to process file type
Trapmine	Unable to process file type
Bkav Pro	—
Trustlook	—

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | RELATIONS | BEHAVIOR

No security vendors flagged this file as malicious

Community Score

2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c

SwissIO_Fixed.zip

2026-03-10 00:30:56 UTC

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

Indicators

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Dropped Info

Non malicious dropped files (3)

/root/.cache/dconf/user
File type: data
96A296D224F285C67BEE93C30F8A309157F0DAA35DC5B87E410B78630A09CFC7

/var/log/auth.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 48478
44A3BAB2C338E3BCA24C00F7C3DA1301EB4A5A889F1C667CC781E1BDACD3B9E7

/var/log/kern.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 2025890
AC941EAD01D5451A7A9FD4BE4BA9B60B2D3E4138670AE868E655B3B393253227

Overview
Indicators
Mitre Attack
Dropped Info
Processes Extra Info
Screenshots

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**
None

Process: logrotate PID: **4942** Parent PID: **4880**
None

Process: logrotate PID: **4947** Parent PID: **4880**
None

Process: logrotate PID: **4945** Parent PID: **4880**
None

Process: logrotate PID: **4946** Parent PID: **4880**
None

Process: exo-open PID: **4993** Parent PID: **4989**
None

Process: exo-open PID: **4991** Parent PID: **4989**
None

Process: sh PID: **4943** Parent PID: **4942**
None

Process: sh PID: **4948** Parent PID: **4947**
None

Process: exo-open PID: **4994** Parent PID: **4993**
None

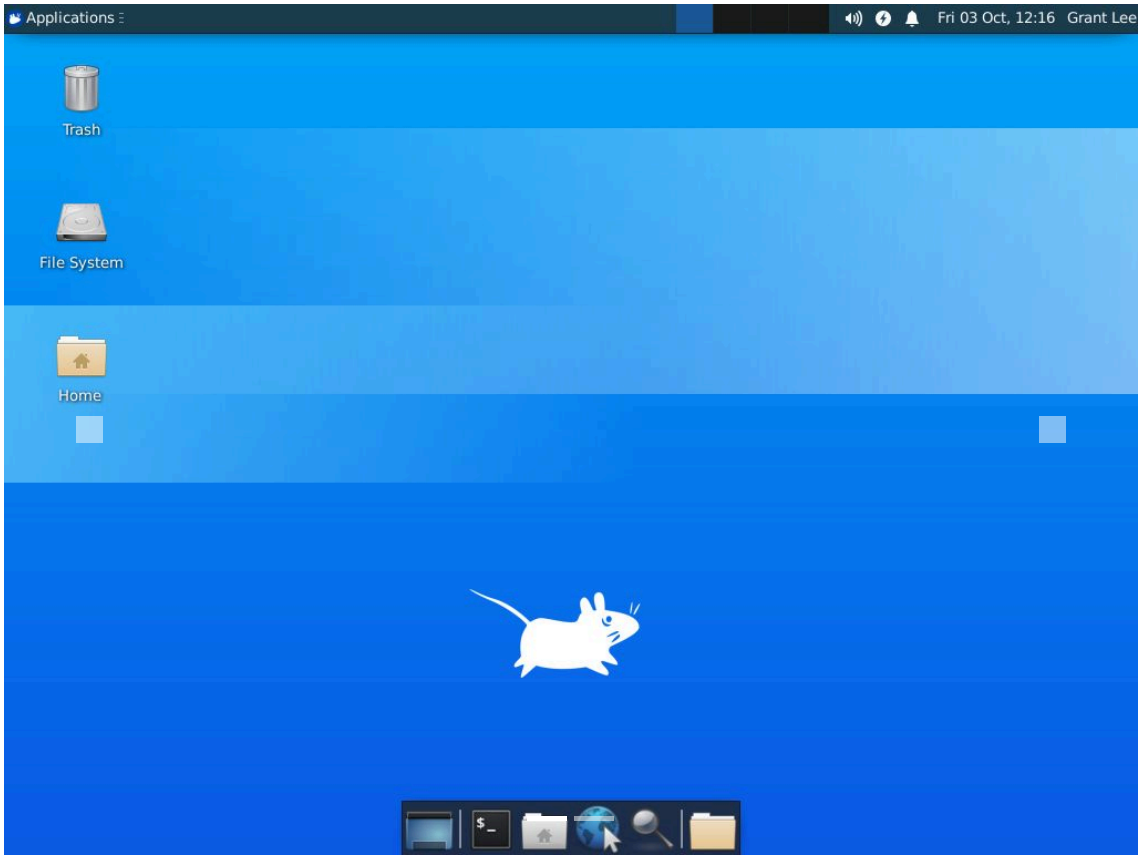
Process: rsyslog-rotate PID: **4944** Parent PID: **4943**
None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**
None

Process: engrampa PID: **5005** Parent PID: **4994**
None

Process: engrampa PID: **4997** Parent PID: **4994**
None

Screenshots



VIRUSTOTAL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Display grouped sandbox reports

Zenbox Linux	0	5	0	0	2	0

Activity Summary

Download Artifacts Full Reports Help

Detections

NOT FOUND

Mitre Signatures

6 INFO

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

1 GZIP

Network comms

NOT FOUND

Behavior Tags

detect-debug-environment sets-process-name

MITRE ATT&CK Tactics and Techniques

Search for technique, subtechnique and in its matching entries

None Info

Execution
TA0002 1 Techniques

Scripting
T1064

1

Persistence
TA0003 2 Techniques

Create or Modify S
T1543

Behavior Similarity Hashes

Zenbox Linux… 532dd8d49eff2a3d52b4084223ac6797

File system actions

Files Opened

/dev/urandom
/etc/dconf/profile/user
/etc/fonts/conf.avail
/etc/fonts/conf.avail/10-antialias.conf
/etc/fonts/conf.avail/10-autohint.conf
/etc/fonts/conf.avail/10-hinting-full.conf
/etc/fonts/conf.avail/10-hinting-medium.conf
/etc/fonts/conf.avail/10-hinting-none.conf
/etc/fonts/conf.avail/10-hinting-slight.conf
/etc/fonts/conf.avail/10-no-sub-pixel.conf

Files Written

/root/.cache/dconf/user

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Files Dropped

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Process and service actions

Processes Created

- /bin/gzip
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
- /usr/bin/exo-open -
- /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
- /usr/bin/systemctl systemctl kill -s HUP rsyslog.service
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate

Shell Commands

- /bin/gzip
- /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh engrampa /tmp/SwissIO_Fixed.zip
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate
- 7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- engrampa /tmp/SwissIO_Fixed.zip
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- systemctl kill -s HUP rsyslog.service

Processes Tree

- 4989 - /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
  - 4991 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
  - 4993 - /usr/bin/exo-open -
- 4994 - /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
  - 4997 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --

close-stderr

5005 - /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip

4942 - /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog

4943 - /usr/lib/rsyslog/rsyslog-rotate

4944 - /usr/bin/systemctl systemctl kill -s HUP rsyslog.service

4945 - /bin/gzip

Highlighted actions

Highlighted Text

""

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

/root/.cache/dconf/user
File type: data
96A296D224F285C67BEE93C30F8A309157F0DAA35DC5B87E410B78630A09CFC7

/var/log/auth.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 48478
44A3BAB2C338E3BCA24C00F7C3DA1301EB4A5A889F1C667CC781E1BDACD3B9E7

/var/log/kern.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 2025890
AC941EAD01D5451A7A9FD4BE4BA9B60B2D3E4138670AE868E655B3B393253227

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

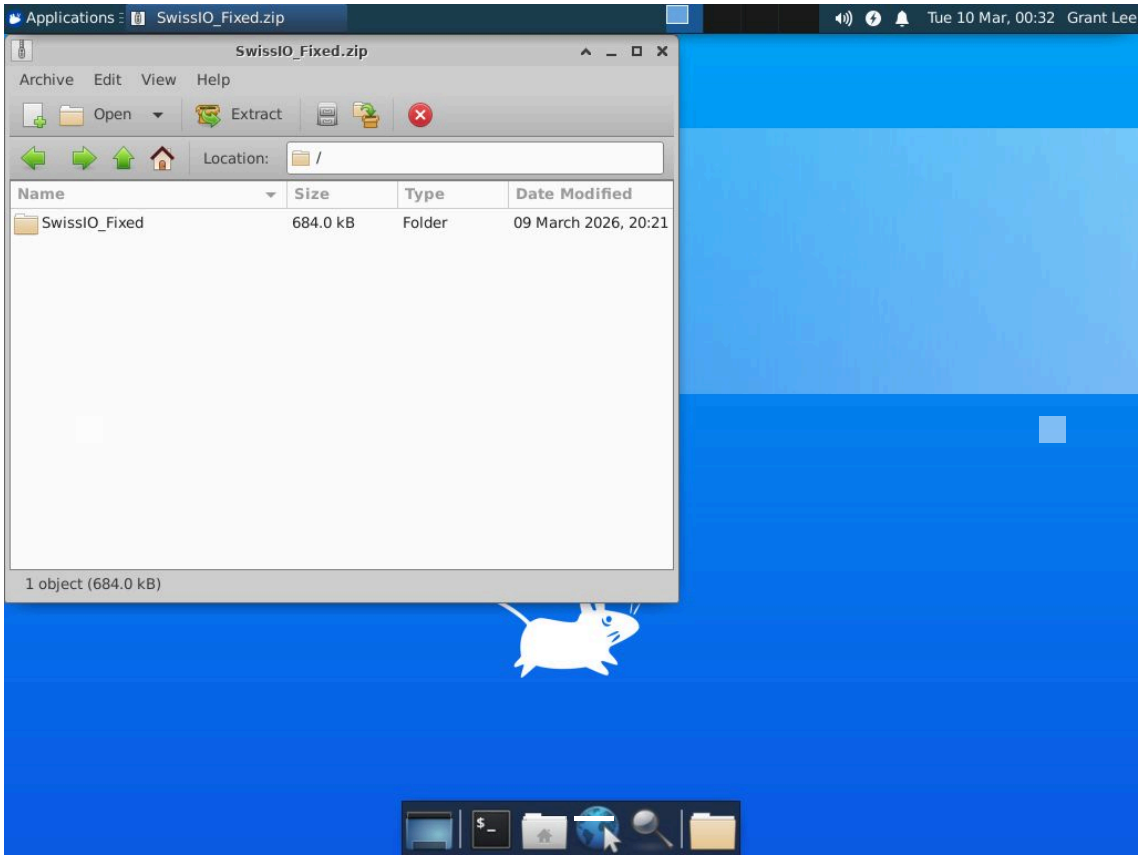
None

Overview

Overview

Indicators
Mitre Attack
Dropped Info
Processes
Extra Info
Screenshots

Screenshots



- Overview
- Indicators
- Mitre Attack
- Dropped Info
- Processes Extra Info
- Screenshots

Overview

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

Indicators

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

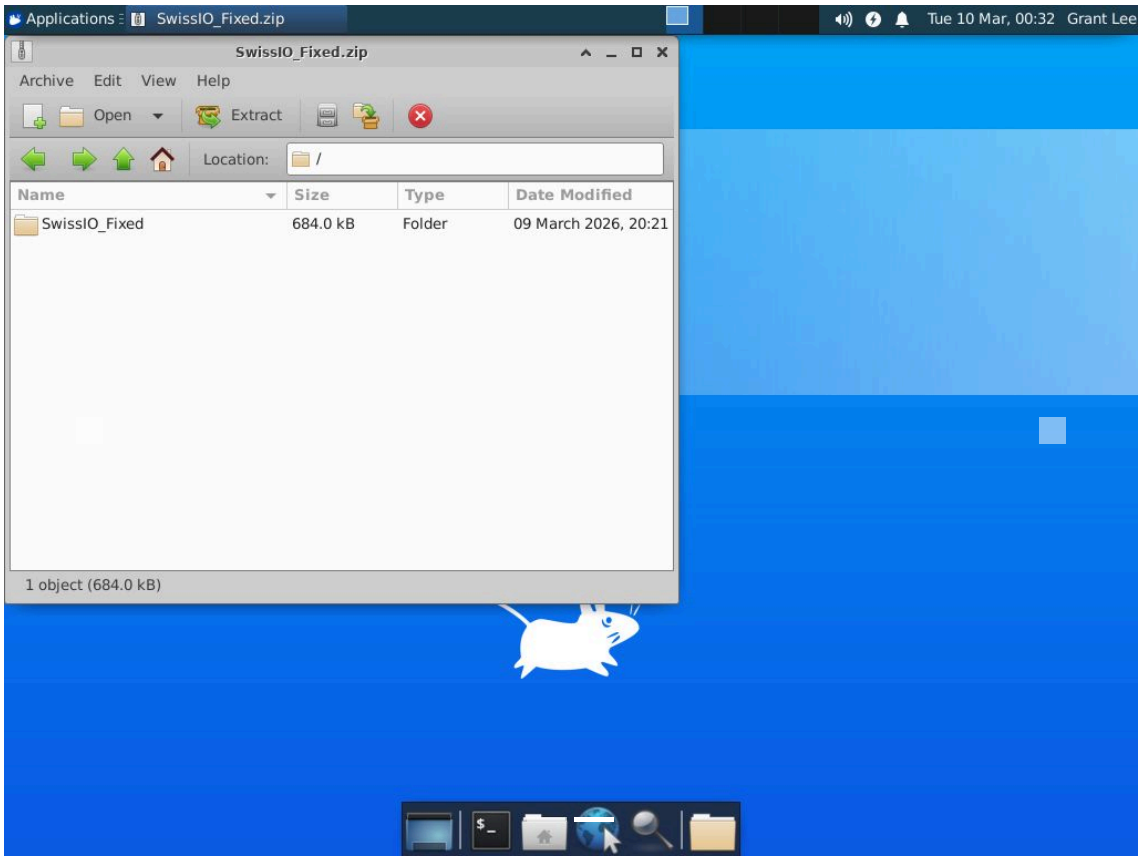
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots


Applications
SwissIO_Fixed.zip
Tue 10 Mar, 00:32
Grant Lee
SwissIO_Fixed.zip
Archive
Edit
View
Help
Open
Extract
Location:
/
Name
Size
Type
Date Modified
SwissIO_Fixed
684.0 kB
Folder
09 March 2026, 20:21
1 object (684.0 kB)

Overview
Indicators
Mitre Attack
Dropped Info
Processes Extra Info
Screenshots

Zenbox Linux Verdict

2/100

File Info

File name:	SwissIO_Fixed.zip
File	Zip archive data, at least v1.0 to extract, compression
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

Overview

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

Indicators

System Summary (1)

0.0 Classification label

Persistence and Installation Behavior (3)

1.0 Executes commands using a shell command-line interpreter

1.0 Executes the "systemctl" command used for controlling the systemd system and service manager

1.0 Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0 Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

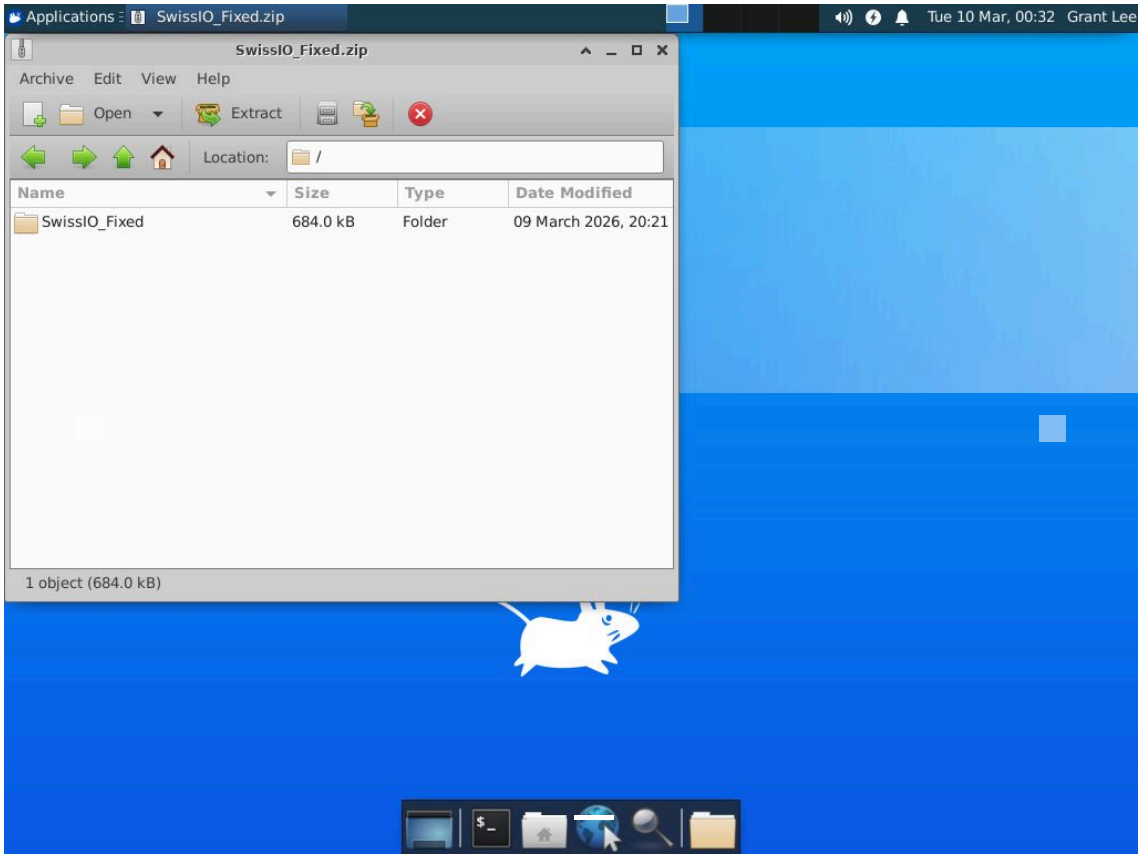
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots


Applications
SwissIO_Fixed.zip
Tue 10 Mar, 00:32
Grant Lee
SwissIO_Fixed.zip
Archive
Edit
View
Help
Open
Extract
Location:
/
Name
Size
Type
Date Modified
SwissIO_Fixed
684.0 kB
Folder
09 March 2026, 20:21
1 object (684.0 kB)

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

Indicators

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

- Overview
- Indicators
- Mitre Attack
- Dropped Info
- Processes Extra Info
- Screenshots

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Overview

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

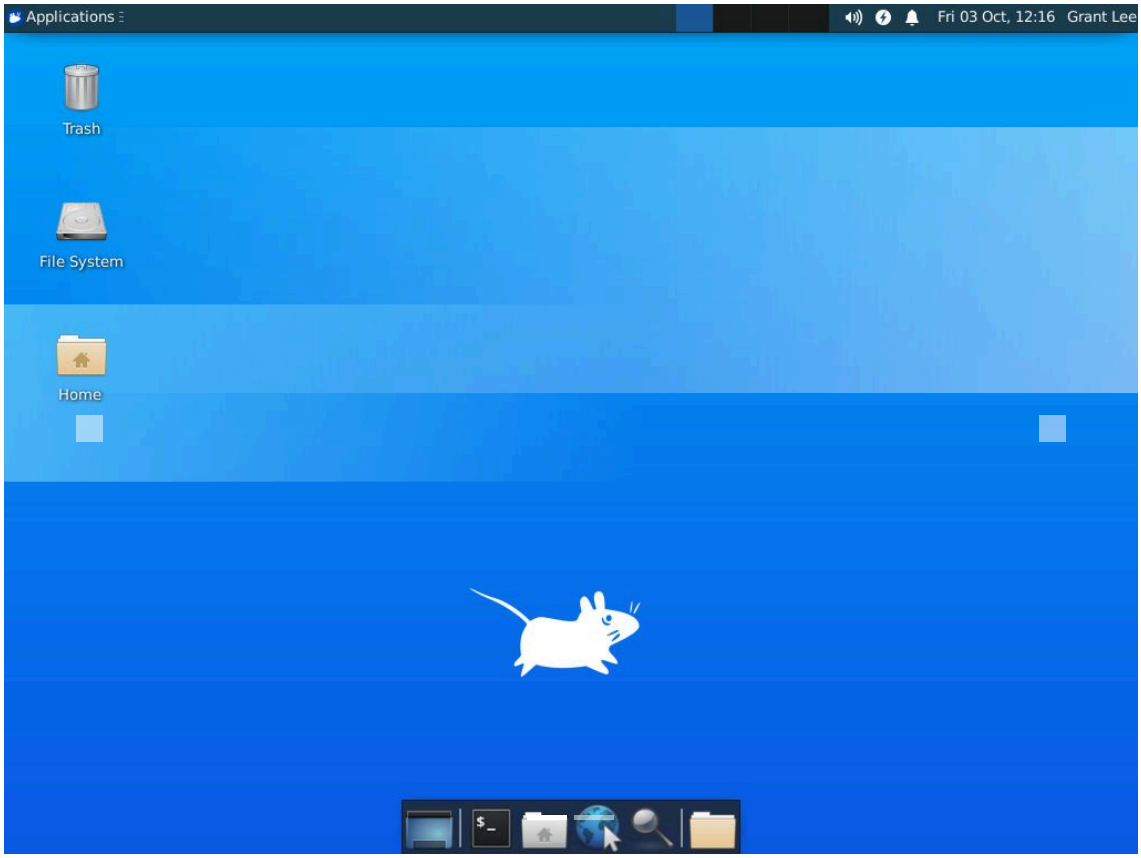
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots


Applications
Fri 03 Oct, 12:16 Grant Lee
Trash
File System
Home

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots

Overview

Overview

Indicators

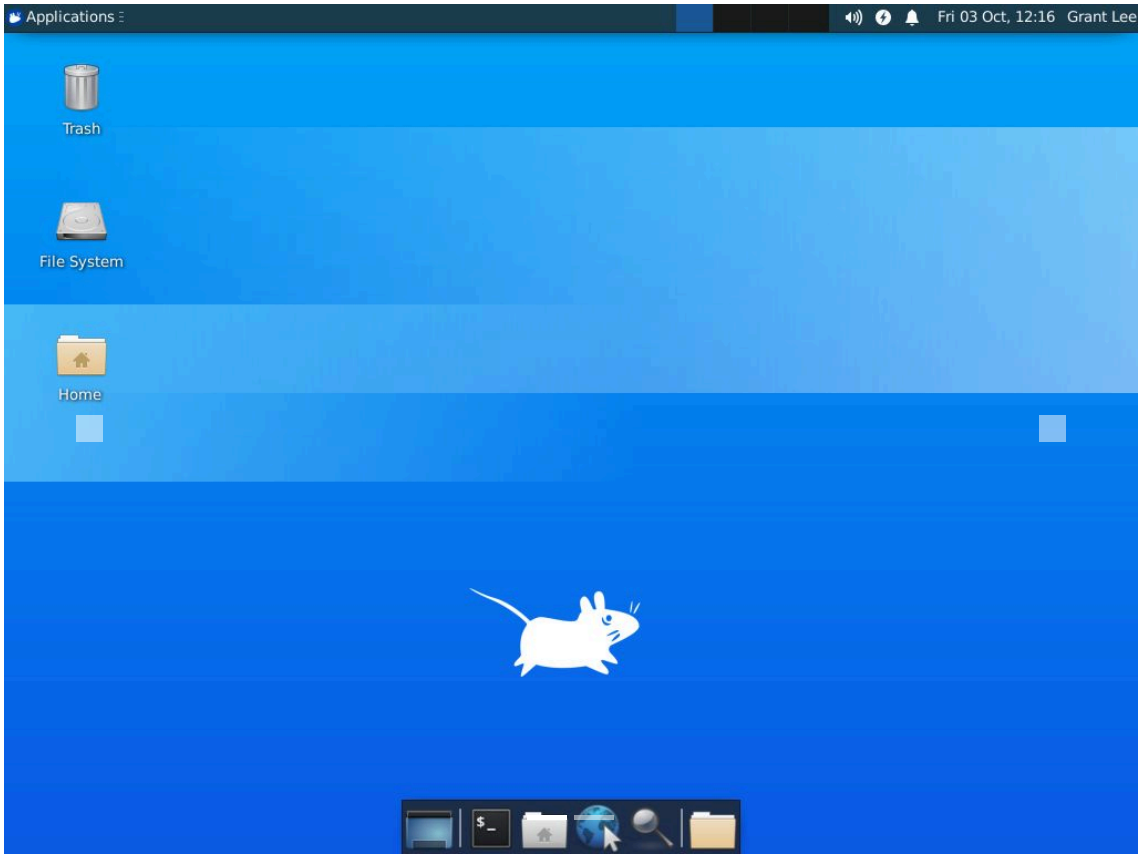
Mitre Attack

Dropped Info

Processes

Extra Info

Screenshots



Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Mitre Attack

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

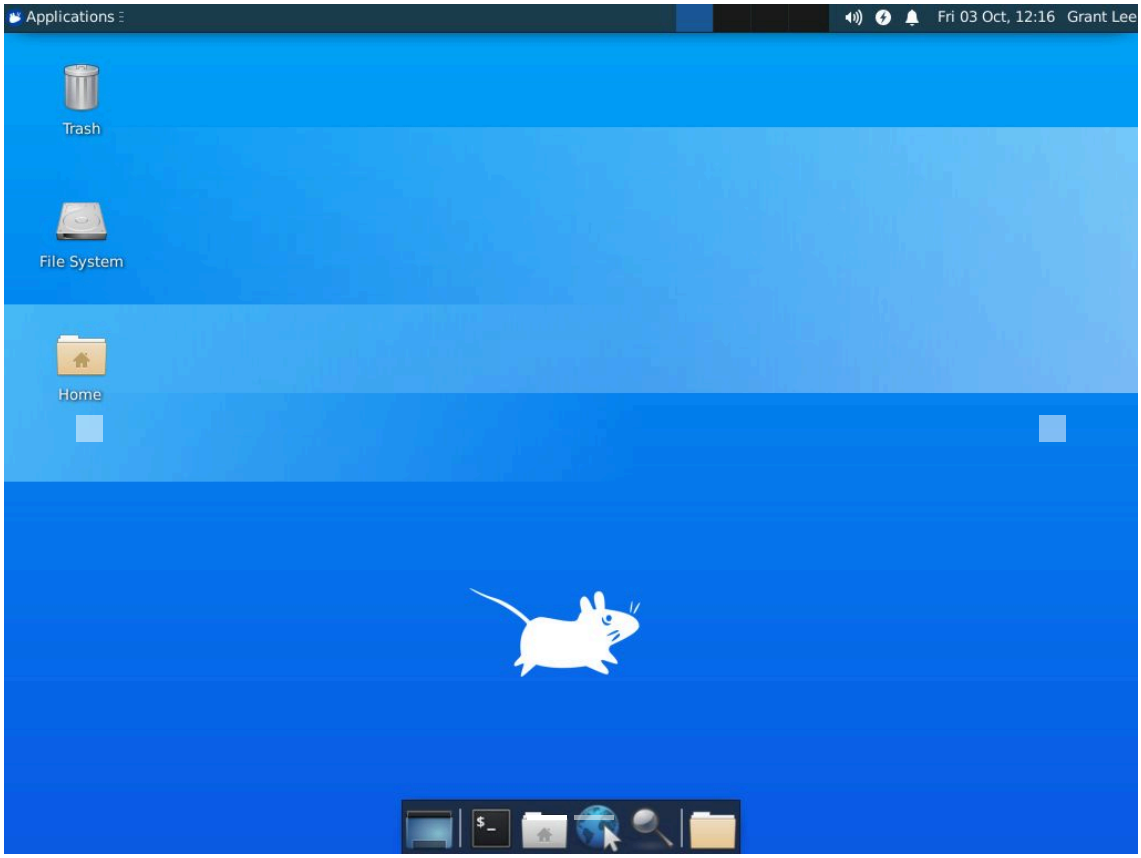
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots



Overview

Indicators

Mitre Attack

Dropped Info

Processes Extra Info

Screenshots

Overview

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Mitre Attack

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

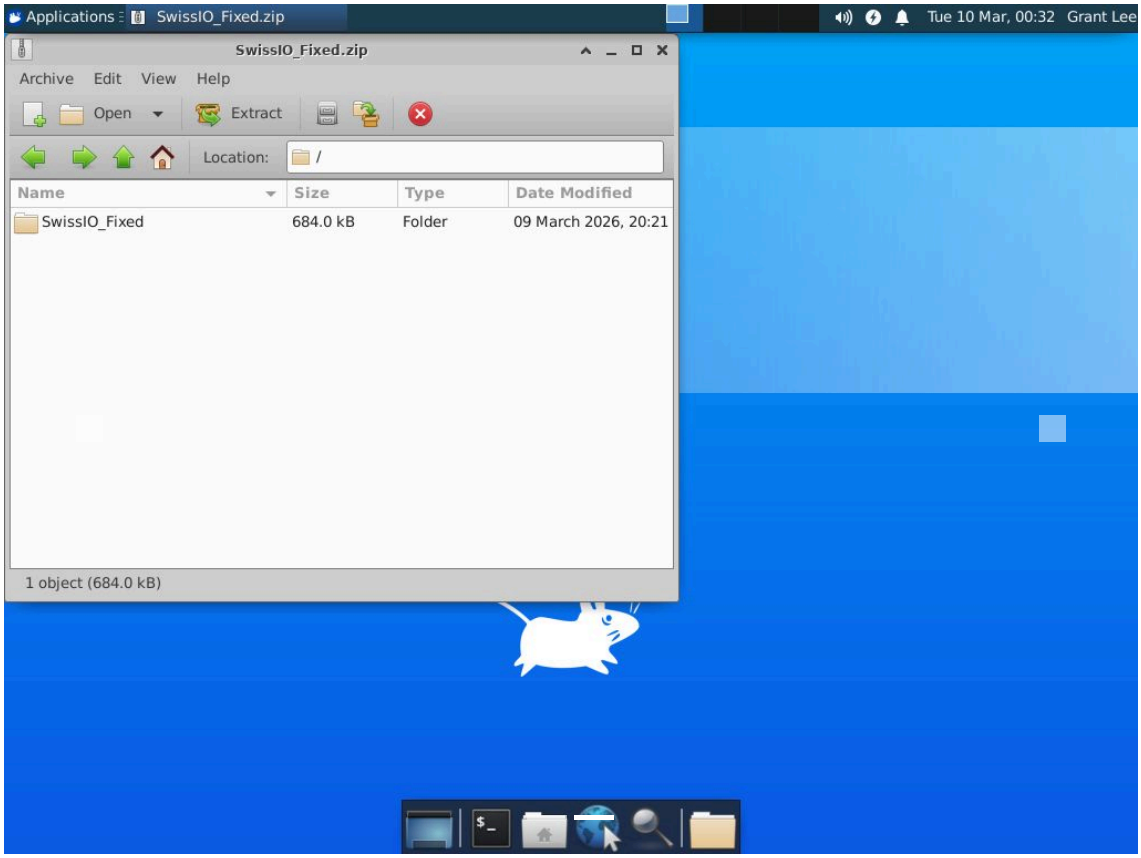
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots



Overview

Indicators

Mitre Attack

Dropped Info

Processes
Extra Info

Screenshots

Overview

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Mitre Attack

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

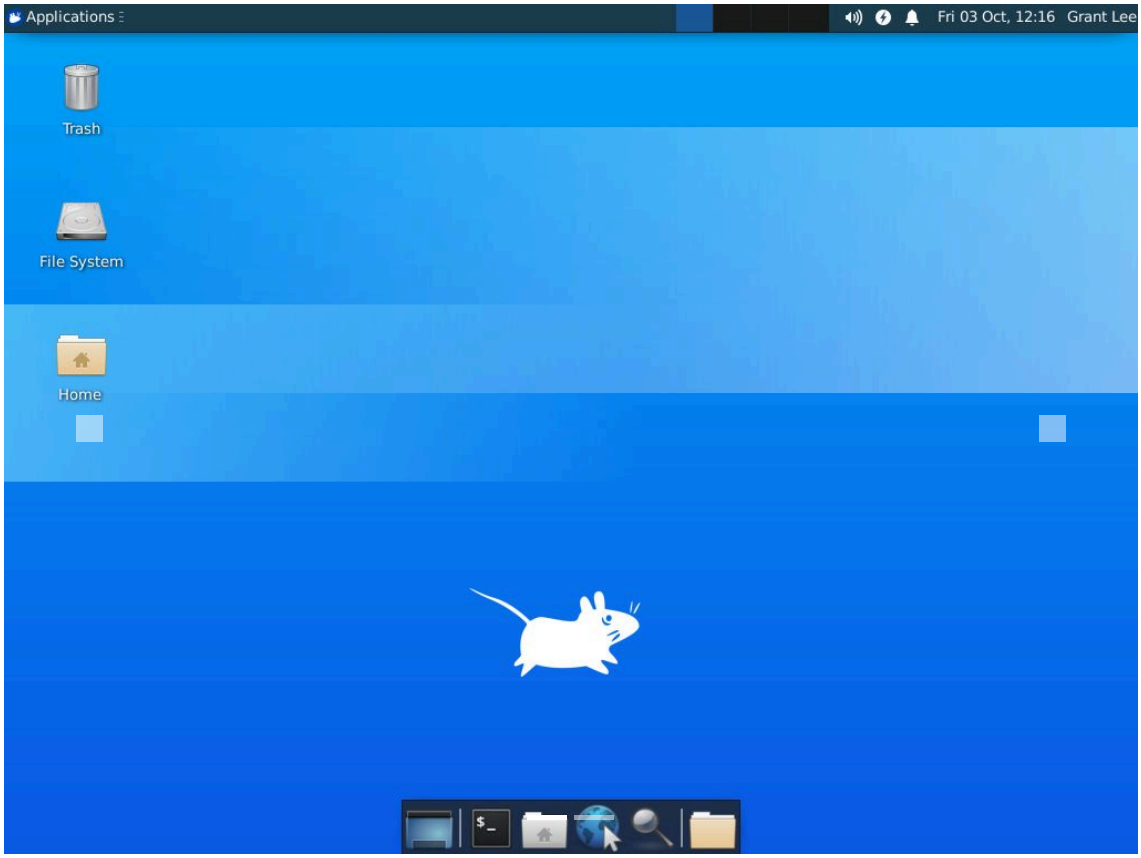
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots



Overview

Indicators

Mitre Attack

Dropped Info

Processes Extra Info

Screenshots

Overview

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

Indicators

Overview
Indicators
Mitre Attack
Dropped Info
Processes Extra Info
Screenshots

Overview

0.0 Classification label

Persistence and Installation Behavior (3)

1.0 Executes commands using a shell command-line interpreter

1.0 Executes the "systemctl" command used for controlling the systemd system and service manager

1.0 Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0 Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting confidence: medium

Persistence

- T1543.002 Systemd Service confidence: medium
- T1064 Scripting confidence: medium

Privilege Escalation

- T1543.002 Systemd Service confidence: medium

Defense Evasion

- T1564.001 Hidden Files and Directories confidence: medium

Discovery

- T1518.001 Security Software Discovery confidence: medium

Dropped Info

Non malicious dropped files (3)

/root/.cache/dconf/user
File type: data
96A296D224F285C67BEE93C30F8A309157F0DAA35DC5B87E410B78630A09CFC7

/var/log/auth.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 48478
44A3BAB2C338E3BCA24C00F7C3DA1301EB4A5A889F1C667CC781E1BDACD3B9E7

/var/log/kern.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 2025890
AC941EAD01D5451A7A9FD4BE4BA9B60B2D3E4138670AE868E655B3B393253227

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

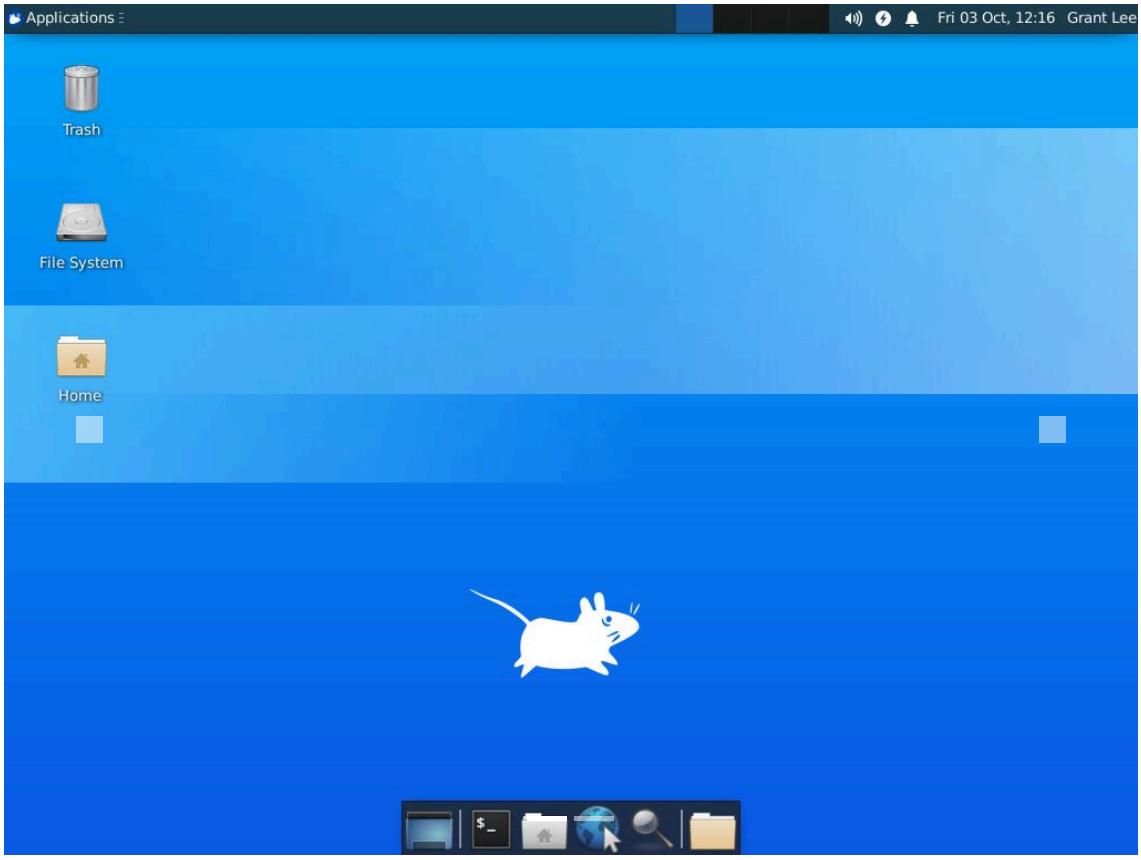
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots



Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Mitre Attack

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

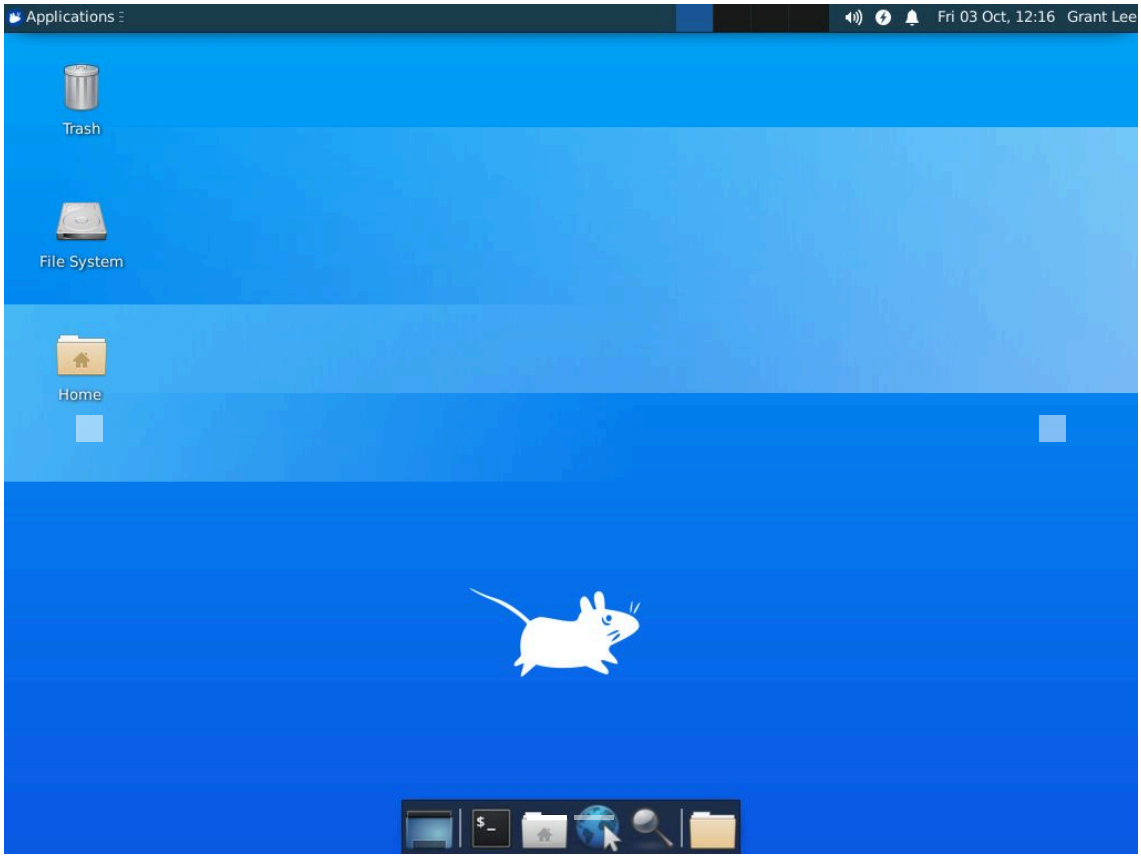
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots



Overview

Indicators

Mitre Attack

Dropped Info

Processes Extra Info

Screenshots

Overview

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Mitre Attack

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

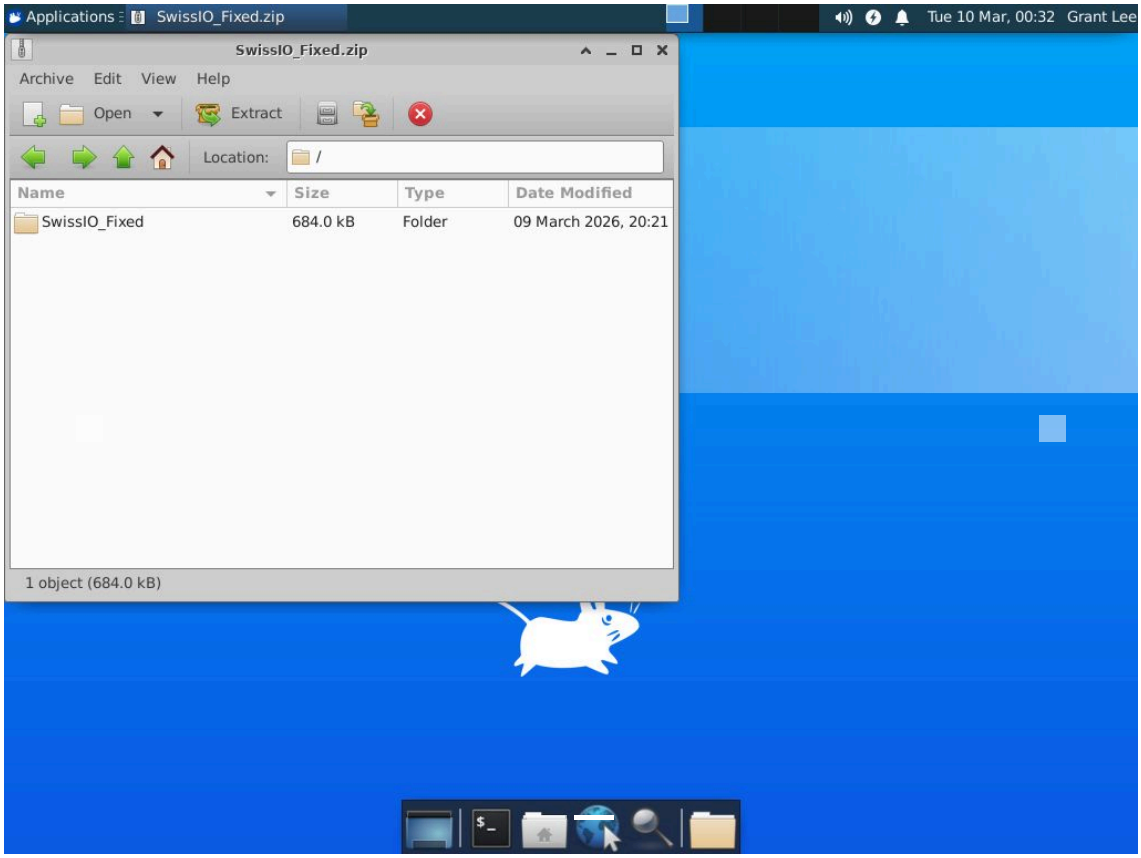
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots



Overview

Indicators

Mitre Attack

Dropped Info

Processes
Extra Info

Screenshots

Overview

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Mitre Attack

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

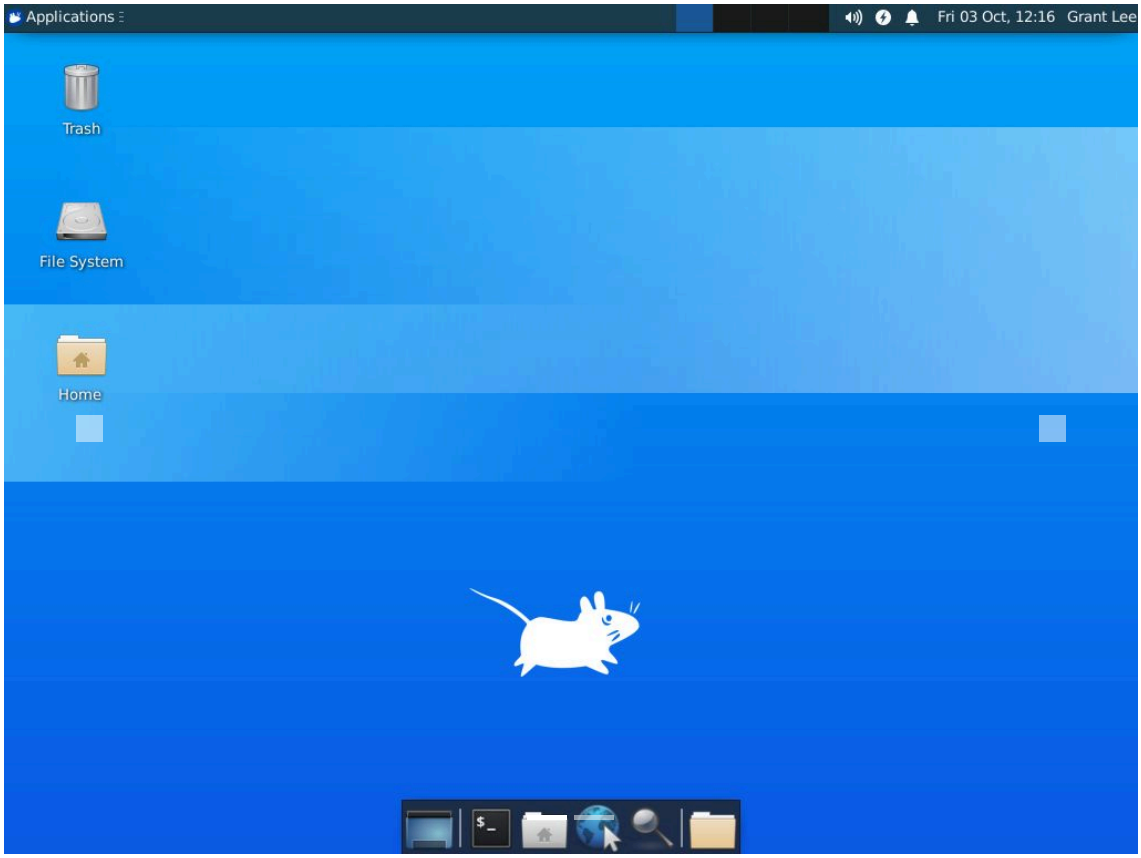
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots



Overview

Indicators

Mitre Attack

Dropped Info

Processes Extra Info

Screenshots

Overview

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots

Overview

Overview

Indicators

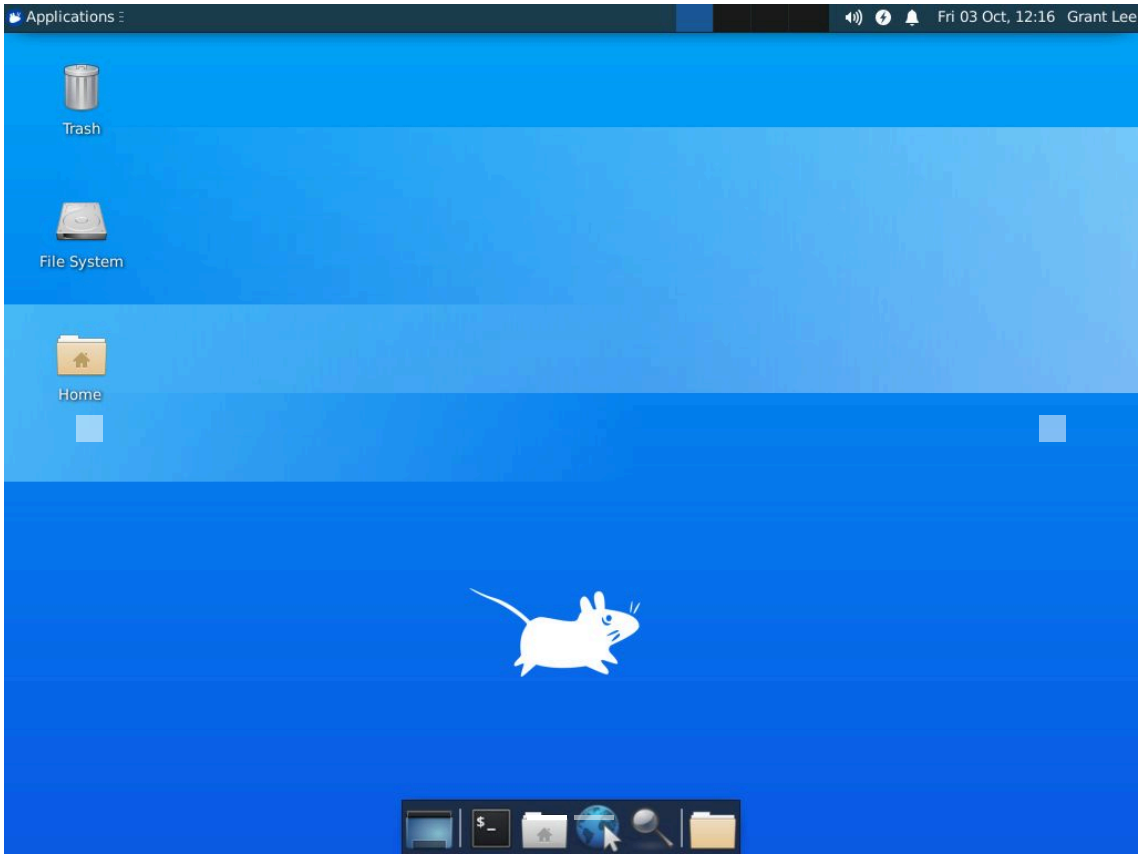
Mitre Attack

Dropped Info

Processes

Extra Info

Screenshots



Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

Indicators

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

- Overview
- Indicators
- Mitre Attack
- Dropped Info
- Processes Extra Info
- Screenshots

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Overview

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

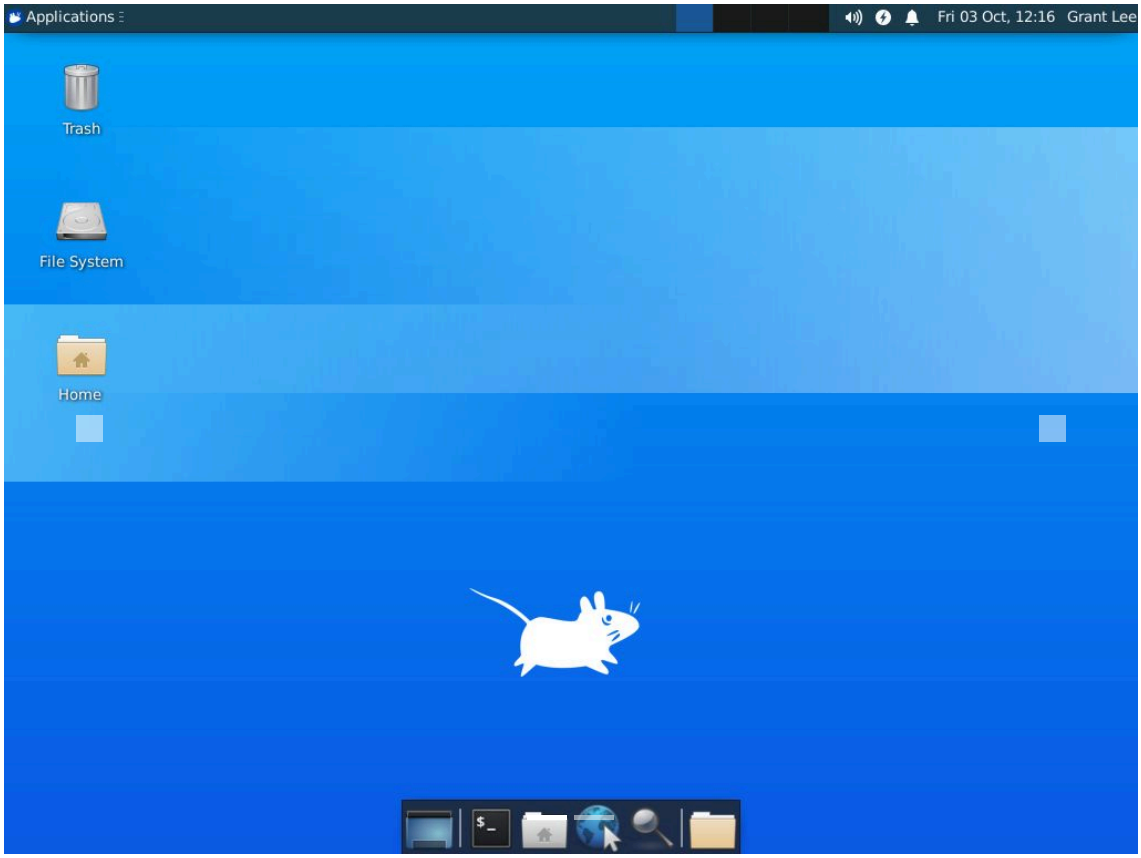
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots


Applications
Fri 03 Oct, 12:16 Grant Lee
Trash
File System
Home

Overview
Indicators
Mitre Attack
Dropped Info
Processes Extra Info
Screenshots

Zenbox Linux Verdict

2/100

File Info

File name:	SwissIO_Fixed.zip
File	Zip archive data, at least v1.0 to extract, compression
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

Overview

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

Indicators

System Summary (1)

0.0 Classification label

Persistence and Installation Behavior (3)

1.0 Executes commands using a shell command-line interpreter

1.0 Executes the "systemctl" command used for controlling the systemd system and service manager

1.0 Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0 Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

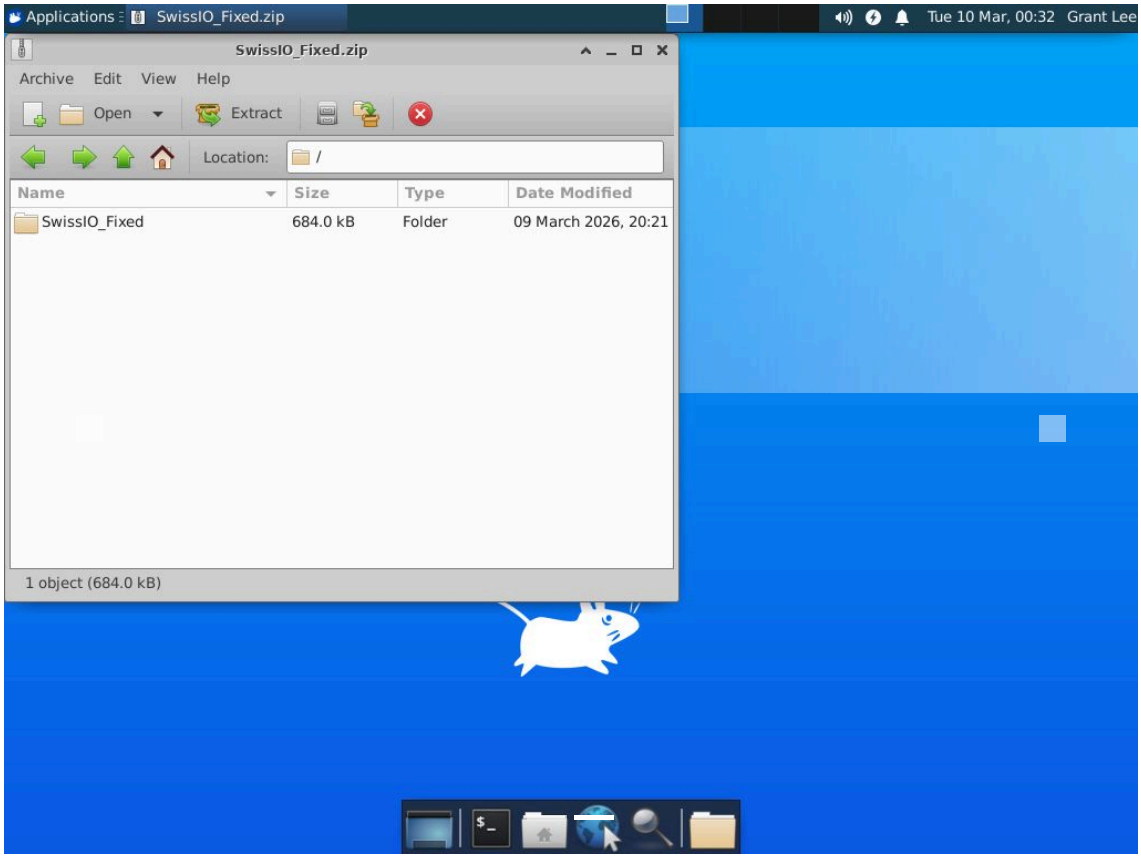
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots


Applications
SwissIO_Fixed.zip
Tue 10 Mar, 00:32
Grant Lee
SwissIO_Fixed.zip
Archive
Edit
View
Help
Open
Extract
Location:
/
Name
Size
Type
Date Modified
SwissIO_Fixed
684.0 kB
Folder
09 March 2026, 20:21
1 object (684.0 kB)

- Overview
- Indicators
- Mitre Attack
- Dropped Info
- Processes Extra Info
- Screenshots

Overview

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

Indicators

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Dropped Info

Non malicious dropped files (3)

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

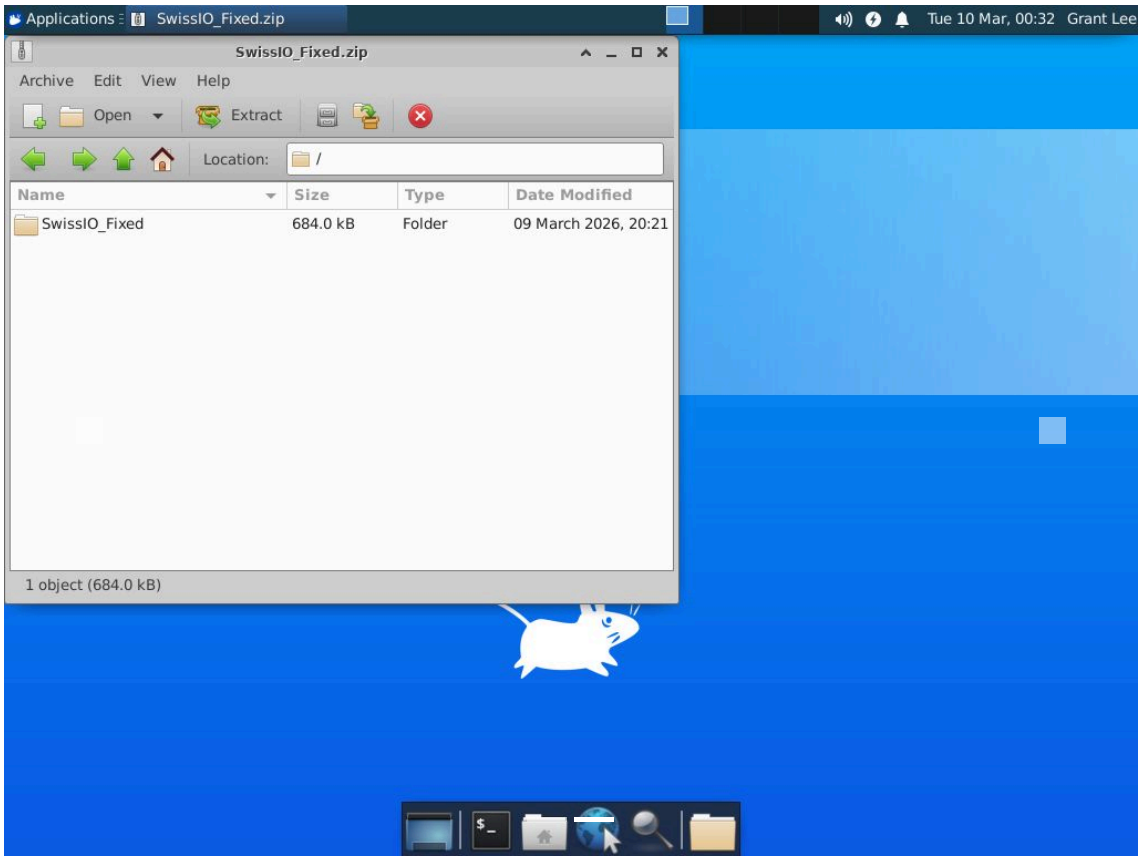
Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots


Applications
SwissIO_Fixed.zip
Tue 10 Mar, 00:32
Grant Lee
SwissIO_Fixed.zip
Archive
Edit
View
Help
Open
Extract
Location:
/
Name
Size
Type
Date Modified
SwissIO_Fixed
684.0 kB
Folder
09 March 2026, 20:21
1 object (684.0 kB)

Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

Indicators

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Dropped Info

Non malicious dropped files (3)

/root/.cache/dconf/user
File type: data
96A296D224F285C67BEE93C30F8A309157F0DAA35DC5B87E410B78630A09CFC7

/var/log/auth.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 48478
44A3BAB2C338E3BCA24C00F7C3DA1301EB4A5A889F1C667CC781E1BDACD3B9E7

/var/log/kern.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 2025890
AC941EAD01D5451A7A9FD4BE4BA9B60B2D3E4138670AE868E655B3B393253227

Overview
Indicators
Mitre Attack
Dropped Info
Processes Extra Info
Screenshots

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**
None

Process: logrotate PID: **4942** Parent PID: **4880**
None

Process: logrotate PID: **4947** Parent PID: **4880**
None

Process: logrotate PID: **4945** Parent PID: **4880**
None

Process: logrotate PID: **4946** Parent PID: **4880**
None

Process: exo-open PID: **4993** Parent PID: **4989**
None

Process: exo-open PID: **4991** Parent PID: **4989**
None

Process: sh PID: **4943** Parent PID: **4942**
None

Process: sh PID: **4948** Parent PID: **4947**
None

Process: exo-open PID: **4994** Parent PID: **4993**
None

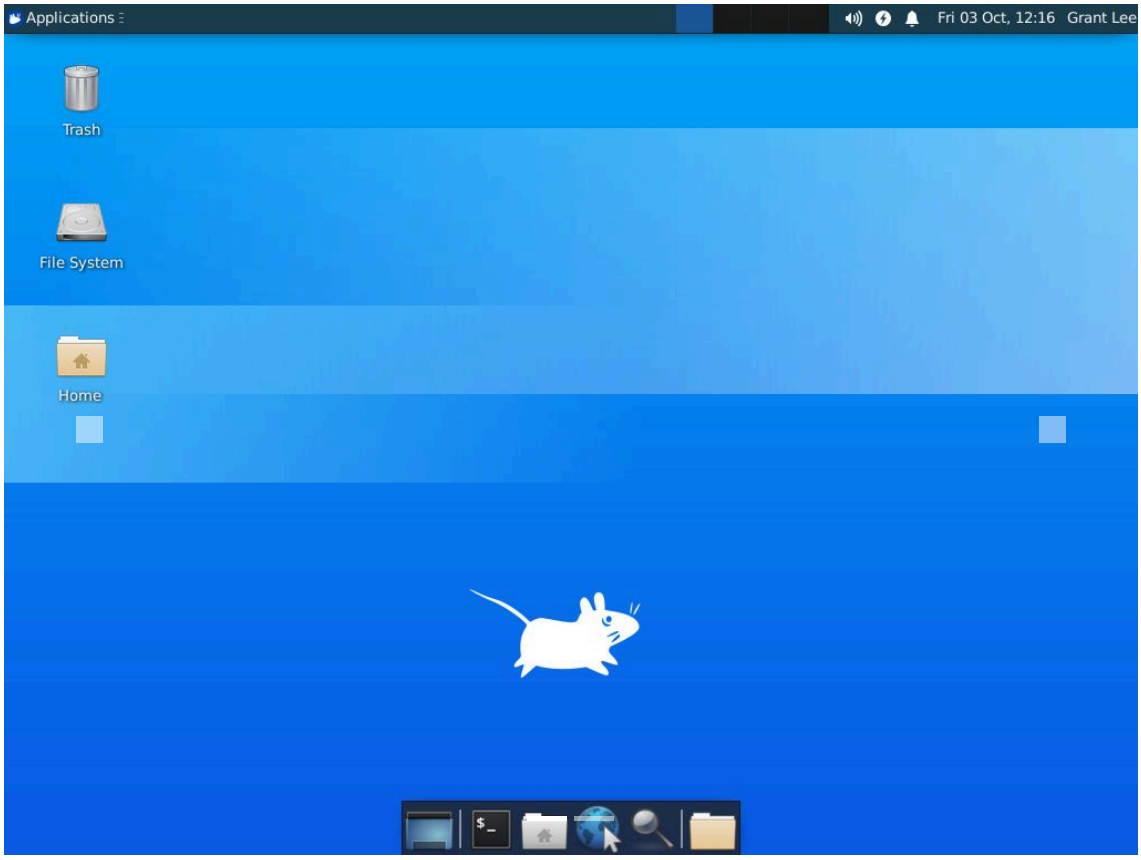
Process: rsyslog-rotate PID: **4944** Parent PID: **4943**
None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**
None

Process: engrampa PID: **5005** Parent PID: **4994**
None

Process: engrampa PID: **4997** Parent PID: **4994**
None

Screenshots



Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Indicators

Dropped Info

Non malicious dropped files (3)

/root/.cache/dconf/user
File type: data
96A296D224F285C67BEE93C30F8A309157F0DAA35DC5B87E410B78630A09CFC7

/var/log/auth.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 48478
44A3BAB2C338E3BCA24C00F7C3DA1301EB4A5A889F1C667CC781E1BDACD3B9E7

/var/log/kern.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 2025890
AC941EAD01D5451A7A9FD4BE4BA9B60B2D3E4138670AE868E655B3B393253227

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

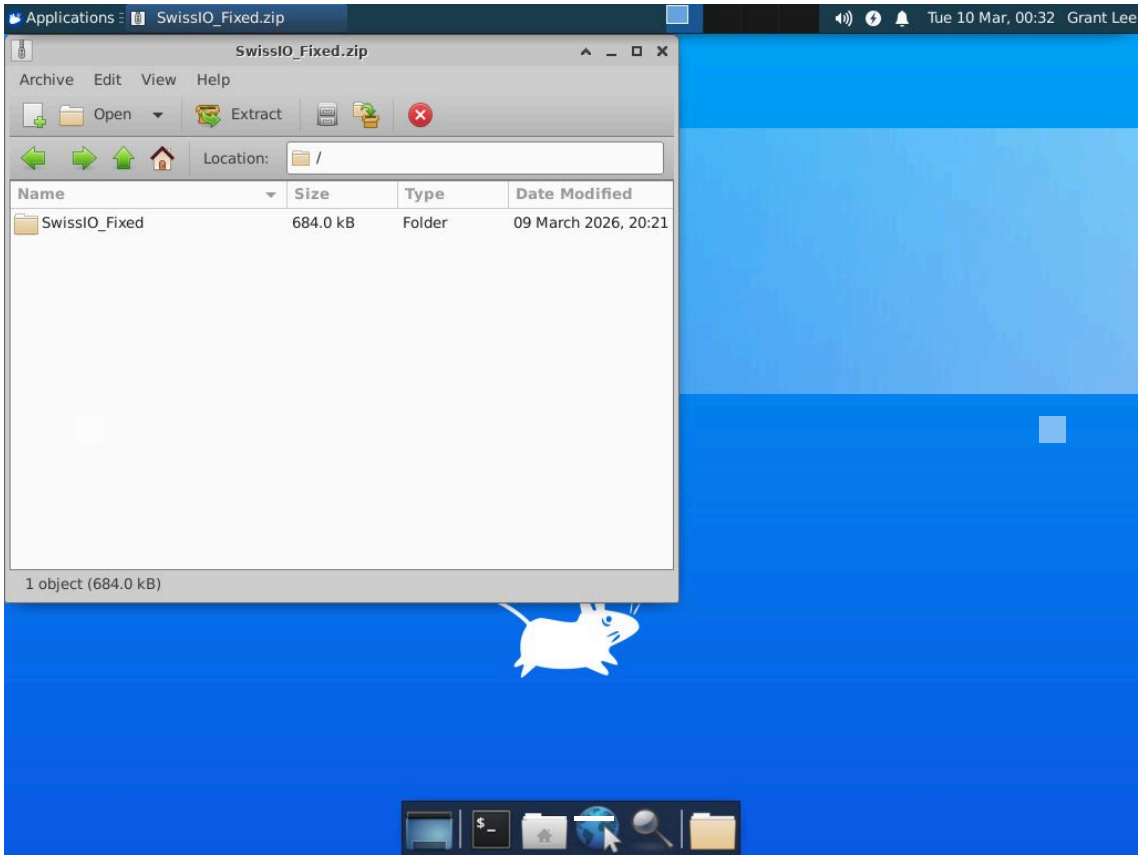
None

Overview

Overview

Indicators
Mitre Attack
Dropped Info
Processes
Extra Info
Screenshots

Screenshots



VIRUSTOTAL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Display grouped sandbox reports

Zenbox Linux	0	5	0	0	2	0

Activity Summary

Download Artifacts Full Reports Help

Detections

NOT FOUND

Mitre Signatures

6 INFO

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

1 GZIP

Network comms

NOT FOUND

Behavior Tags

detect-debug-environment sets-process-name

MITRE ATT&CK Tactics and Techniques

Search for technique, subtechnique and in its matching entries

None Info

Execution
TA0002 1 Techniques

Scripting
T1064

1

Persistence
TA0003 2 Techniques

Create or Modify S
T1543

Behavior Similarity Hashes

Zenbox Linux… 532dd8d49eff2a3d52b4084223ac6797

File system actions

Files Opened

/dev/urandom
/etc/dconf/profile/user
/etc/fonts/conf.avail
/etc/fonts/conf.avail/10-antialias.conf
/etc/fonts/conf.avail/10-autohint.conf
/etc/fonts/conf.avail/10-hinting-full.conf
/etc/fonts/conf.avail/10-hinting-medium.conf
/etc/fonts/conf.avail/10-hinting-none.conf
/etc/fonts/conf.avail/10-hinting-slight.conf
/etc/fonts/conf.avail/10-no-sub-pixel.conf

Files Written

/root/.cache/dconf/user

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Files Dropped

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Process and service actions

Processes Created

- /bin/gzip
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
- /usr/bin/exo-open -
- /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
- /usr/bin/systemctl systemctl kill -s HUP rsyslog.service
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate

Shell Commands

- /bin/gzip
- /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh engrampa /tmp/SwissIO_Fixed.zip
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate
- 7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- engrampa /tmp/SwissIO_Fixed.zip
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- systemctl kill -s HUP rsyslog.service

Processes Tree

- 4989 - /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
  - 4991 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
  - 4993 - /usr/bin/exo-open -
- 4994 - /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
  - 4997 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --

close-stderr

5005 - /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip

4942 - /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog

4943 - /usr/lib/rsyslog/rsyslog-rotate

4944 - /usr/bin/systemctl systemctl kill -s HUP rsyslog.service

4945 - /bin/gzip

Highlighted actions

Highlighted Text

""

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | RELATIONS | BEHAVIOR

No security vendors flagged this file as malicious

Community Score

2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c

SwissIO_Fixed.zip

2026-03-10 00:30:56 UTC

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | RELATIONS | BEHAVIOR

Security vendors' analysis	Do you want to automate checks?
Acronis (Static ML)	Undetected
AhnLab-V3	Undetected
Alibaba	Undetected
AliCloud	Undetected
ALYac	Undetected
Antiy-AVL	Undetected
Arcabit	Undetected
Avast	Undetected
Avast-Mobile	Undetected
AVG	Undetected
Avira (no cloud)	Undetected
Baidu	Undetected
BitDefender	Undetected
ClamAV	Undetected
CMC	Undetected
CrowdStrike Falcon	Undetected
CTX	Undetected
Cynet	Undetected
DrWeb	Undetected
Emsisoft	Undetected
eScan	Undetected
ESET-NOD32	Undetected
Fortinet	Undetected
GData	Undetected
Google	Undetected
Gridinsoft (no cloud)	Undetected
Huorong	Undetected
Ikarus	Undetected
Jiangmin	Undetected
K7AntiVirus	Undetected
K7GW	Undetected
Kaspersky	Undetected

Kingsoft	Undetected
Lionic	Undetected
Malwarebytes	Undetected
MaxSecure	Undetected
McAfee Scanner	Undetected
Microsoft	Undetected
NANO-Antivirus	Undetected
Panda	Undetected
QuickHeal	Undetected
Rising	Undetected
Sangfor Engine Zero	Undetected
Skyhigh (SWG)	Undetected
Sophos	Undetected
SUPERAntiSpyware	Undetected
Symantec	Undetected
TACHYON	Undetected
Tencent	Undetected
Trellix ENS	Undetected
TrendMicro	Undetected
TrendMicro-HouseCall	Undetected
Varist	Undetected
VBA32	Undetected
VIPRE	Undetected
VirIT	Undetected
ViRobot	Undetected
Webroot	Undetected
WithSecure	Undetected
Xcitium	Undetected
Yandex	Undetected
Zillya	Undetected
ZoneAlarm by Check Point	Undetected
Zoner	Undetected
Arctic Wolf	Unable to process file type
BitDefenderFalx	Unable to process file type
DeepInstinct	Unable to process file type
Elastic	Unable to process file type
Palo Alto Networks	Unable to process file type
SecureAge	Unable to process file type
SentinelOne (Static ML)	Unable to process file type

Symantec Mobile Insight	Unable to process file type
TEHTRIS	Unable to process file type
Trapmine	Unable to process file type
Bkav Pro	—
Trustlook	—

VIRUSTOTAL

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Display grouped sandbox reports

Zenbox Linux	0	5	0	0	2	0

Detections

NOT FOUND

Mitre Signatures

6 INFO

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

1 GZIP

Network comms

NOT FOUND

Behavior Tags

detect-debug-environment sets-process-name

MITRE ATT&CK Tactics and Techniques

Search for technique, subtechnique and in its matching entries

None Info

Activity Summary

Download Artifacts Full Reports Help

T1064

T1543

Behavior Similarity Hashes

Zenbox Linux… 532dd8d49eff2a3d52b4084223ac6797

File system actions

Files Opened

/dev/urandom
/etc/dconf/profile/user
/etc/fonts/conf.avail
/etc/fonts/conf.avail/10-antialias.conf
/etc/fonts/conf.avail/10-autohint.conf
/etc/fonts/conf.avail/10-hinting-full.conf
/etc/fonts/conf.avail/10-hinting-medium.conf
/etc/fonts/conf.avail/10-hinting-none.conf
/etc/fonts/conf.avail/10-hinting-slight.conf
/etc/fonts/conf.avail/10-no-sub-pixel.conf

Files Written

/root/.cache/dconf/user

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Files Dropped

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Process and service actions

Processes Created

- /bin/gzip
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
- /usr/bin/exo-open -
- /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
- /usr/bin/systemctl systemctl kill -s HUP rsyslog.service
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate

Shell Commands

- /bin/gzip
- /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh engrampa /tmp/SwissIO_Fixed.zip
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate
- 7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- engrampa /tmp/SwissIO_Fixed.zip
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- systemctl kill -s HUP rsyslog.service

Processes Tree

- 4989 - /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
  - 4991 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
  - 4993 - /usr/bin/exo-open -
- 4994 - /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
  - 4997 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --

close-stderr

5005 - /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip

4942 - /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog

4943 - /usr/lib/rsyslog/rsyslog-rotate

4944 - /usr/bin/systemctl systemctl kill -s HUP rsyslog.service

4945 - /bin/gzip

Highlighted actions

Highlighted Text

""

VIRUSTOTAL

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Basic properties

MD5	a79b00afca60508e415fa5dc3a9a305d
SHA-1	b187edae085cb261493c22ccbaf17cadc97f1a3f
SHA-256	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b9463…
Vhash	86a41950068c7578c98f5737e6223624
SSDEEP	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:E…
TLSH	T16BA4AF30D12E7CEDD49E703521C741E7F3A2D7150126B8CA6…
File type	ZIP compressed zip
Magic	Zip archive data, at least v1.0 to extract, compression method=st…
TrID	ZIP compressed archive (100%)
Magika	ZIP
File size	463.50 KB (474624 bytes)

History

First Submissi…	2026-03-10 00:30:56 UTC
Last Submissi…	2026-03-10 00:30:56 UTC
Last Analysis	2026-03-10 00:30:56 UTC
Earliest Conte…	2026-03-09 20:21:12
Latest Conten…	2026-03-09 20:21:12

Names

SwissIO_Fixed.zip

Bundle Info

Contents Metadata

Contained Fil…	316
Uncompresse…	667.93 KB
Earliest Conte…	2026-03-09 20:21:12
Latest Conten…	2026-03-09 20:21:12

Contained Files By Type

HTML	1
SCRIPT	15
DIRECTORY	129
UNKNOWN	171

Contained Files By Extension

RS	1
LOCK	1
HTML	1
SH	1
TXT	1
CSS	1
JS	2
JSON	2
TOML	2
MD	3
PY	11
SAMPLE	14

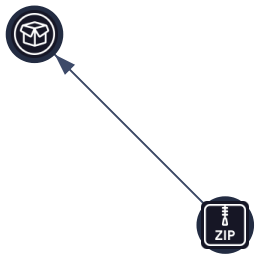
VIRUSTOTAL

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Bundled Files (126)

Scanned	Detections	File type	Name
2026-03-08	0 / 62	Text	SwissIO_Fixed/.git/description
2026-01-18	0 / 60	ZLIB	SwissIO_Fixed/.git/objects/03/d2afd5fe1fb69ca977d620fc564a12b27008aa
2025-12-10	0 / 62	ZLIB	SwissIO_Fixed/.git/objects/d7/b9ef12978379847f8fdf1859d40a76fe1b1b3d
2026-02-28	0 / 62	Perl	SwissIO_Fixed/.git/hooks/fsmonitor-watchman.sample
2026-02-28	0 / 62	Shell script	SwissIO_Fixed/.git/hooks/prepare-commit-msg.sample
2026-02-20	0 / 62	Text	SwissIO_Fixed/.git/HEAD
2026-02-28	0 / 61	Shell script	SwissIO_Fixed/.git/hooks/pre-push.sample
2026-02-28	0 / 62	Shell script	SwissIO_Fixed/.git/hooks/commit-msg.sample
2025-01-12	0 / 60	JavaScript	SwissIO_Fixed/static/addon-fit.min.js
2026-02-28	0 / 62	Shell script	SwissIO_Fixed/.git/hooks/pre-commit.sample

Graph Summary



Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

Indicators

Overview
Indicators
Mitre Attack
Dropped Info
Processes Extra Info
Screenshots

Overview

0.0 Classification label

Persistence and Installation Behavior (3)

1.0 Executes commands using a shell command-line interpreter

1.0 Executes the "systemctl" command used for controlling the systemd system and service manager

1.0 Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0 Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting confidence: medium

Persistence

- T1543.002 Systemd Service confidence: medium
- T1064 Scripting confidence: medium

Privilege Escalation

- T1543.002 Systemd Service confidence: medium

Defense Evasion

- T1564.001 Hidden Files and Directories confidence: medium

Discovery

- T1518.001 Security Software Discovery confidence: medium

Dropped Info

Non malicious dropped files (3)

/root/.cache/dconf/user
File type: data
96A296D224F285C67BEE93C30F8A309157F0DAA35DC5B87E410B78630A09CFC7

/var/log/auth.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 48478
44A3BAB2C338E3BCA24C00F7C3DA1301EB4A5A889F1C667CC781E1BDACD3B9E7

/var/log/kern.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 2025890
AC941EAD01D5451A7A9FD4BE4BA9B60B2D3E4138670AE868E655B3B393253227

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**

None

Process: logrotate PID: **4942** Parent PID: **4880**

None

Process: logrotate PID: **4947** Parent PID: **4880**

None

Process: logrotate PID: **4945** Parent PID: **4880**

None

Process: logrotate PID: **4946** Parent PID: **4880**

None

Process: exo-open PID: **4993** Parent PID: **4989**

None

Process: exo-open PID: **4991** Parent PID: **4989**

None

Process: sh PID: **4943** Parent PID: **4942**

None

Process: sh PID: **4948** Parent PID: **4947**

None

Process: exo-open PID: **4994** Parent PID: **4993**

None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**

None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**

None

Process: engrampa PID: **5005** Parent PID: **4994**

None

Process: engrampa PID: **4997** Parent PID: **4994**

None

Screenshots